NetIQ Access Manager

Op deze pagina vind je hoe je jouw Identity Provider-systeem kunt koppelen aan SURFconext als je gebruik maakt van de NetIQ Access Manager. Het volgende komt hier aan bod:

Stappenplan

Als je jouw Identity Provider-systeem wilt koppelen met NetIQ Access Manager, moet je de volgende stappen doorlopen:

1. Configureer een directory (User Store genoemd) in je Identity Provider-systeem. Deze is nodig voor de identiteiten waarmee je kunt inloggen op SURFconext-diensten.
2. Koppel SURFconext als SAML2.0 Service Provider aan je Identity Provider-systeem (hiermee configureer je jouw systeem ook als Identity Provider). In feite voeg je hierbij de SAML 2.0 metadata van SURFconext toe aan de NetIQ Identity Provider-configuratie.
3. Voeg het SURFconext-‘token signing certificate’ toe aan de ‘Trusted Roots’ van NetIQ Access Manager. Met deze certificaten worden straks SAML 2.0 berichten ondertekend, zodat we zeker weten ze van SURFconext komen en onderweg niet gewijzigd zijn.
4. Geef de metadata-URL van jouw Identity Provider-systeem door aan het SURFconext-team. Het SURFconext-team zorgt ervoor dat de URL wordt opgenomen in de SURFconext-configuratie.
5. Maak een attribute set en mapping aan voor de attributen die je moet meesturen naar SURFconext.
6. Test de configuratie.

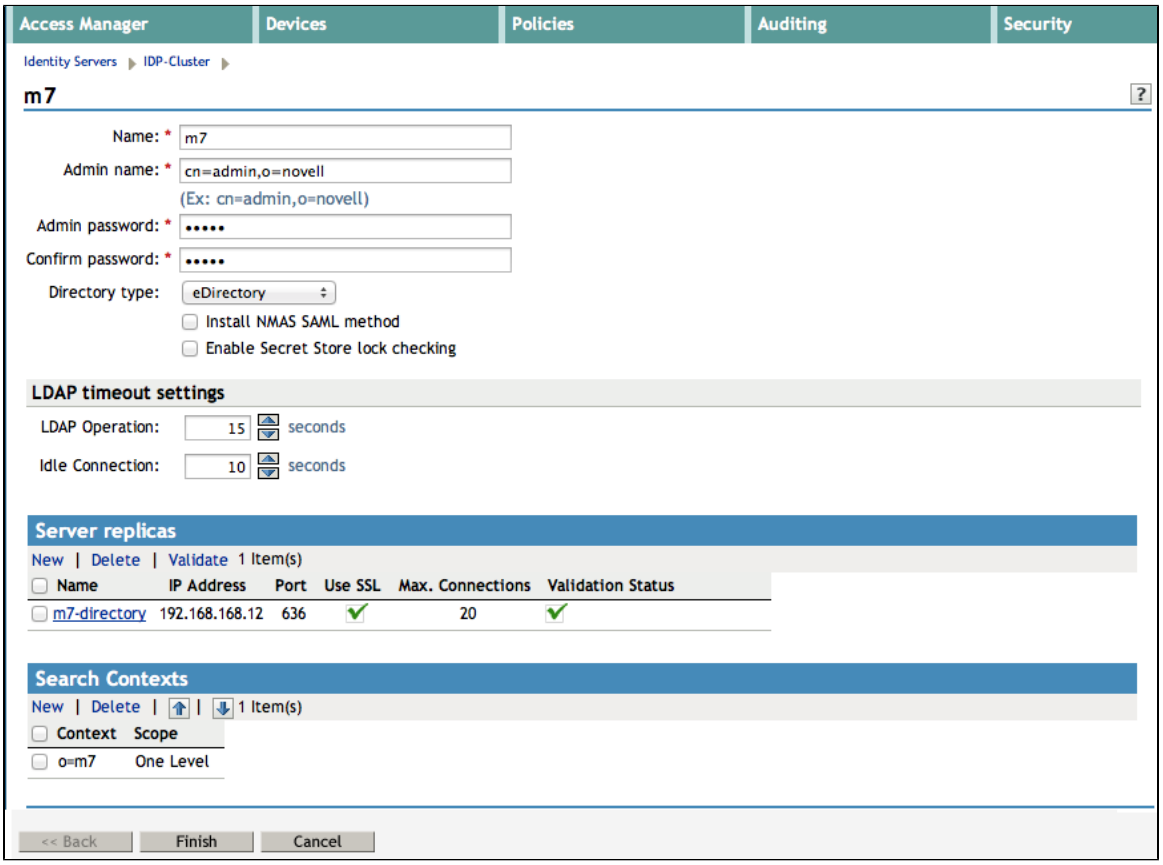
In de tekst hierna wordt per stap uitgelegd, welke acties je moet uitvoeren om bovengenoemde stappen succesvol te doorlopen.

1. User Store toevoegen

Om een User Store-directory te configureren, moet je de volgende stappen doorlopen:

1. Ga naar 'Devices' -> 'Identity Servers' -> 'IDP-cluster’.

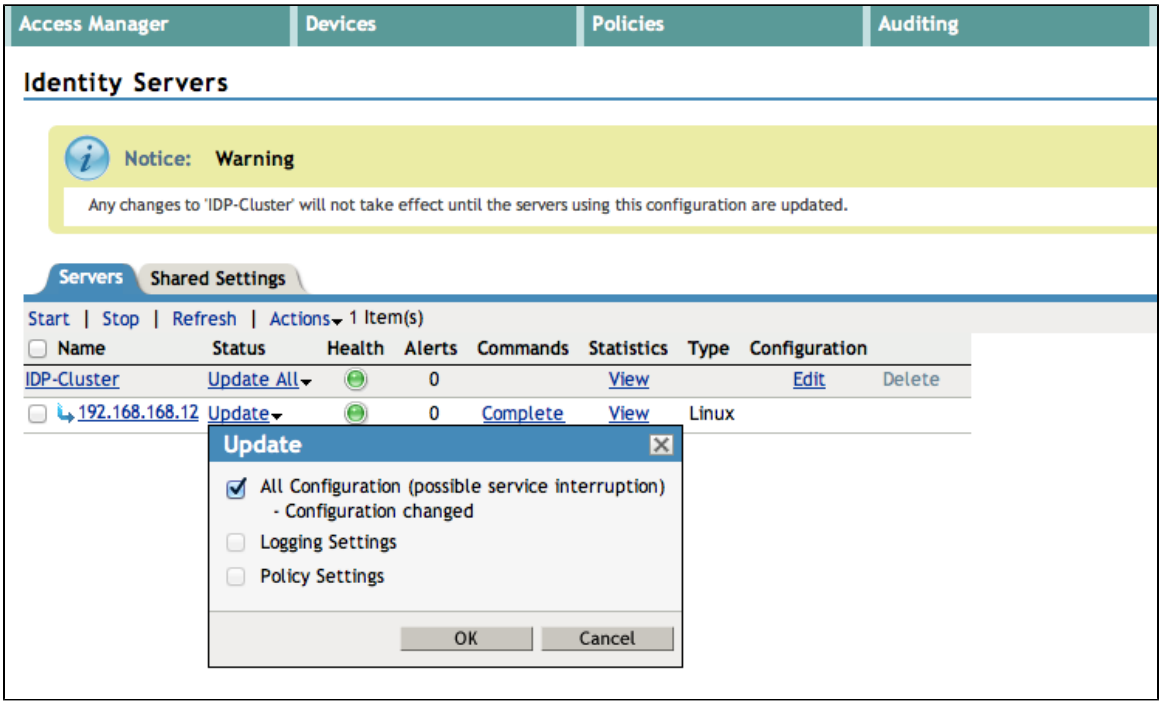
2. Klik in de tab 'Local' onder 'User Stores' op 'New'. Je ziet dan onderstaand scherm:



3. Vul de juiste gegevens in (in ons geval een eDirectory-server van de organisatie 'm7') en klik op 'Finish'.

Merk op dat we een eDirectory replica en een search context (de plek in de directory information tree waaronder iedereen zich bevindt die SURFconext moet kunnen gebruiken; hier kunnen er meerdere van worden opgegeven) hebben gedefinieerd.

4. Update de configuratie onder 'Devices' -> 'Identity Servers' (zie de onderstaande afbeelding). Deze actie onderbreekt de services van Access Manager niet.



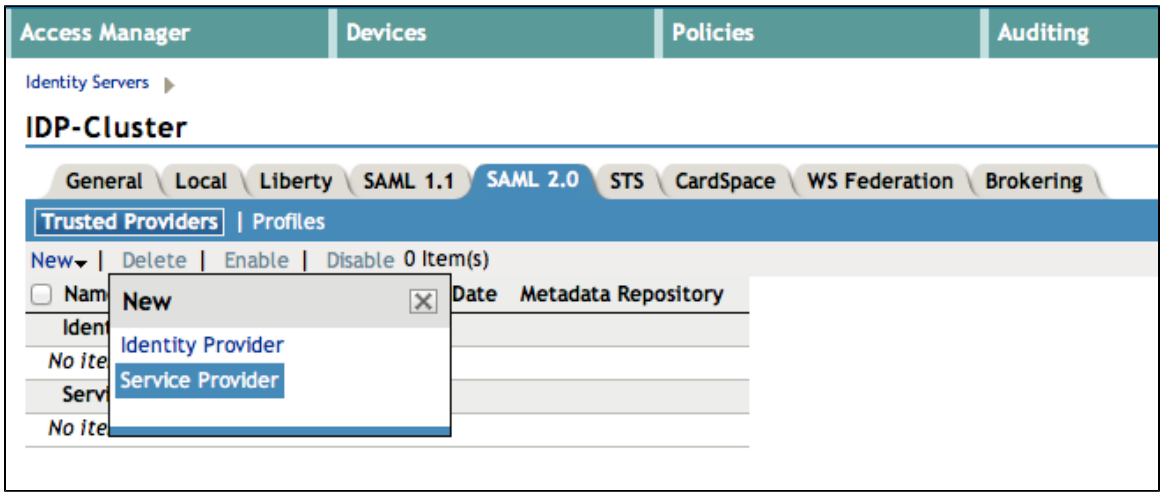
2. SURFconext toevoegen aan de Identity Provider

Om SURFconext toe te voegen aan je Identity Provider-systeem moet je de volgende stappen doorlopen:

1. Ga naar 'Devices' -> 'Identity Servers' -> 'IDP-cluster'.

2. Zet in de tab 'General' onder 'Configuration' onderaan het vinkje bij SAML 2.0 aan.

3. Ga naar de tab 'SAML 2.0'. Kies nu 'New' en dan 'Service Provider' (zie onderstaande figuur).

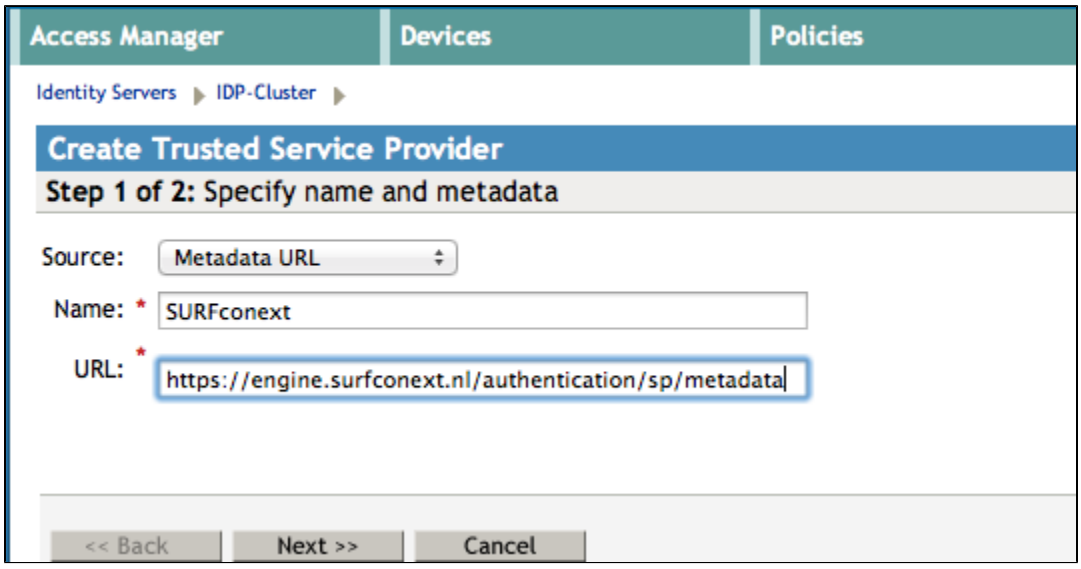


4. Vul de metadata-URL in, zoals je ziet in onderstaande afbeelding. De metadata-URL is:

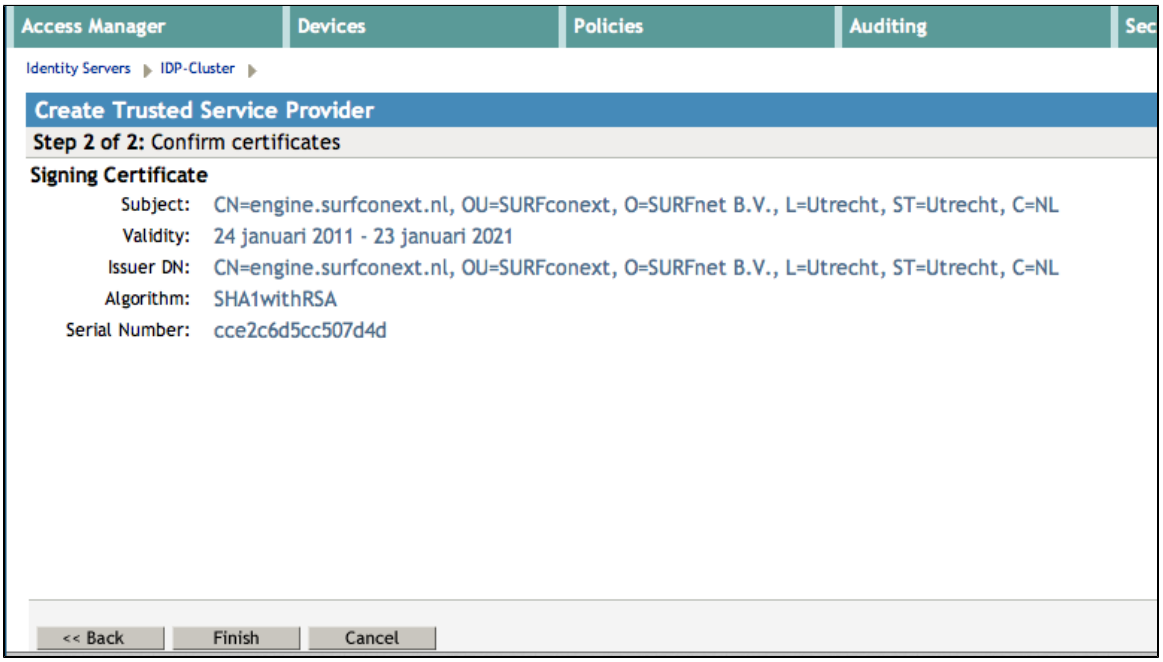
- voor het koppelen aan SURFconext productie: https://metadata.surfconext.nl/sp-metadata.xml
- voor het koppelen aan SURFconext test: https://metadata.test.surfconext.nl/sp-metadata.xml

(de schermafbeelding hieronder vermeldt nog de oude url - gebruik die niet meer). Je voegt hiermee SURFconext toe als Service Provider.

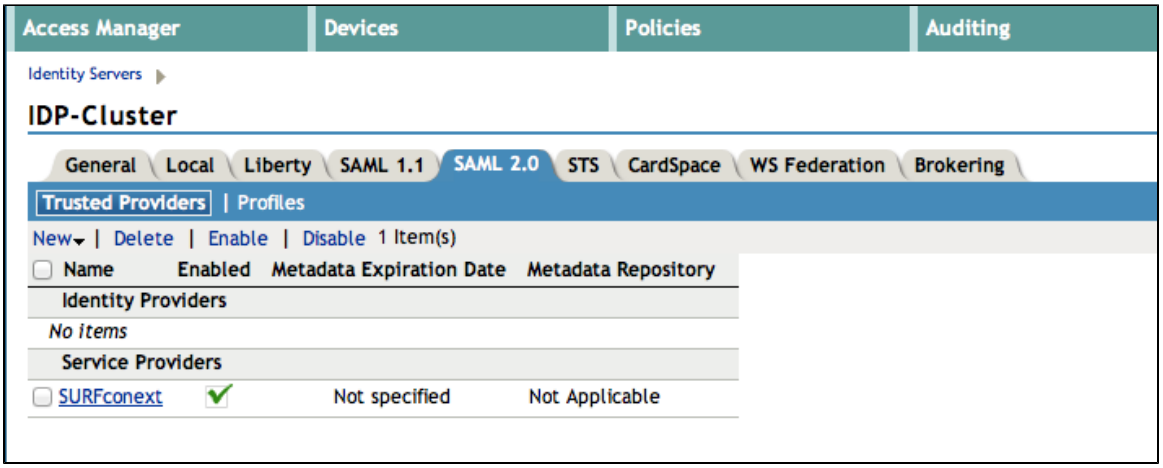
Controleer de URL eerst in een browser en controleer ook het SSL-certificaat bij de URL (de browser geeft dit aan als je op het slotje klikt). Dit is belangrijk omdat je in een later stadium de metadata van SURFconext gaat gebruiken om een trustrelatie met SURFconext op te zetten.



5. Klik op 'Next'. Je ziet dan het volgende:



6. Neem contact op met SURFnet als deze stap mislukt. Als het is gelukt, klik dan op 'Finish'. Je ziet dan het volgende scherm:



7. Update de clusterconfiguratie zoals hierboven beschreven bij stap 4 van de paragraaf 'User store toevoegen'.

3. Voeg het token signing certificate van SURFconext toe

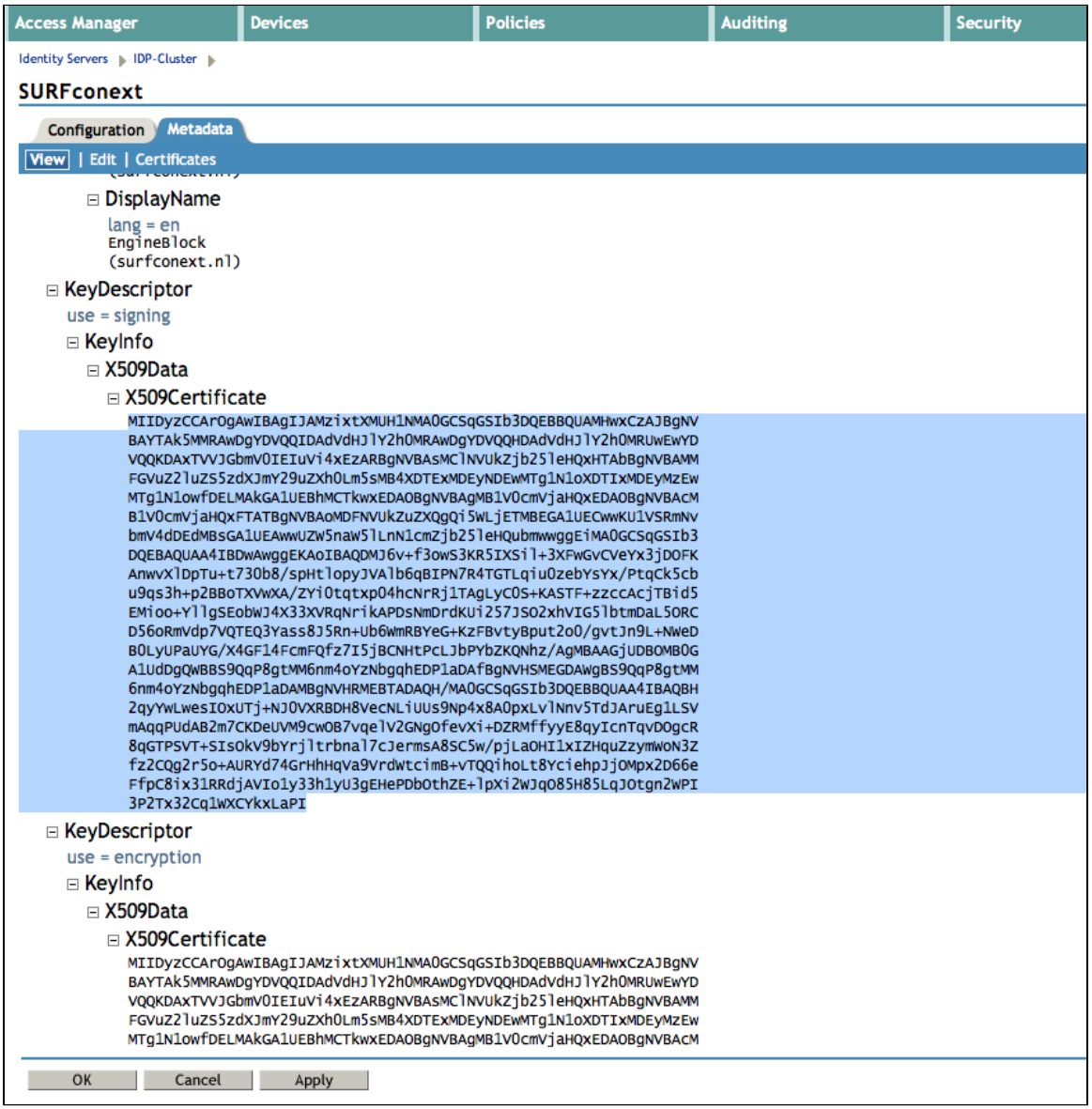
SURFnet gebruikt bij SURFconext zogenaamde self signed tokencertificaten voor het ondertekenen van de SAML 2.0-berichten. Self signed tokencertificaten bieden voldoende garantie omdat SURFconext geen publieke dienst is.

1. Ga naar 'Devices' -> 'Identity Servers' -> 'IDP-cluster'.

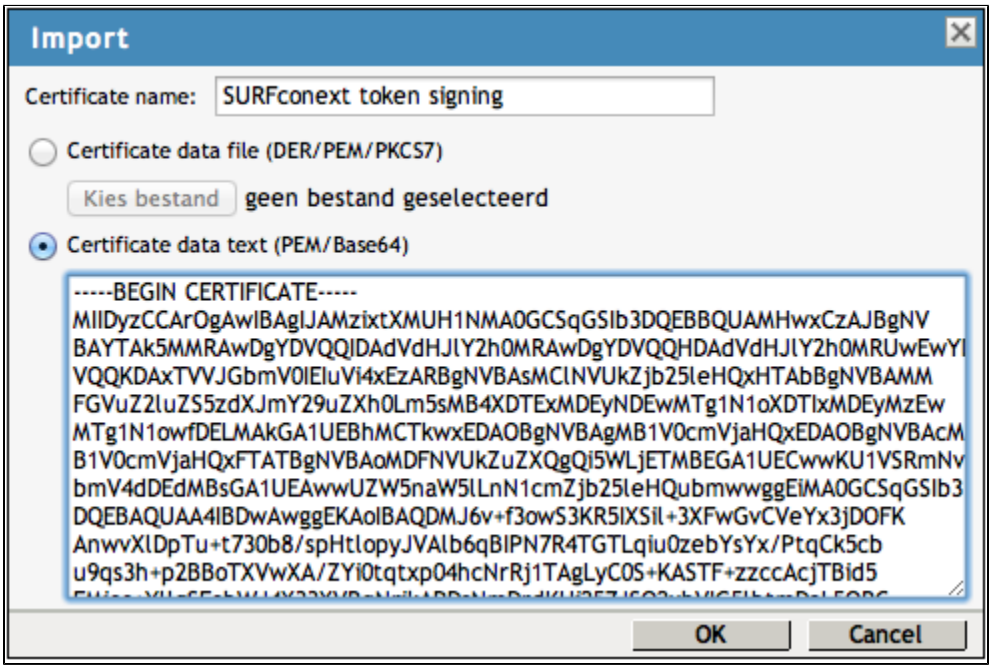
2. Ga naar de tab 'SAML 2.0'. Klik op de zojuist aangemaakte Service Provider.

3. Klik op de tab 'Metadata' en zoek het signing certificate (zie de figuur hieronder).

4. Selecteer en kopieer het singing certificaat zoals dat is gedaan in onderstaand figuur.



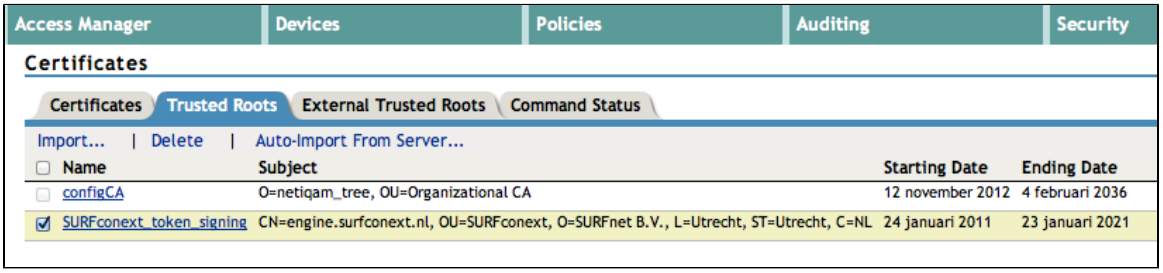
5. Ga nu naar 'Security' -> 'Trusted Roots' en klik op 'import'. Je ziet dan het onderstaande scherm (dat in het voorbeeld al is ingevuld):



Geef het certificaat een beschrijvende naam (hier dus ‘SURFconext token signing’) en selecteer 'Certificate data text'. Plak hierin het gekopieerde certificaat.

6. Voeg in de regel boven het certificaat '-----BEGIN CERTIFICATE-----' toe en in de regel onder het certificaat '-----END CERTIFICATE-----' (dit is niet te zien in de afbeelding hierboven). Hiermee creëer je een geldig PEM-certificaat, zoals NetIQ Access Manager het graag ziet.

7. Klik op 'OK'. Als alles goed is gegaan, zie je het onderstaande scherm:



4. Metadata URL doorgeven aan SURFnet

1. Controleer of op de volgende URL `https://<servernaam>/nidp/saml2/metadata` geldige XML laat zien. Deze metadata bevat alle informatie die nodig is om jouw organisatie aan SURFconext toe te voegen.

> ⚠ Deze URL moet ook voor SURFnet benaderbaar zijn.

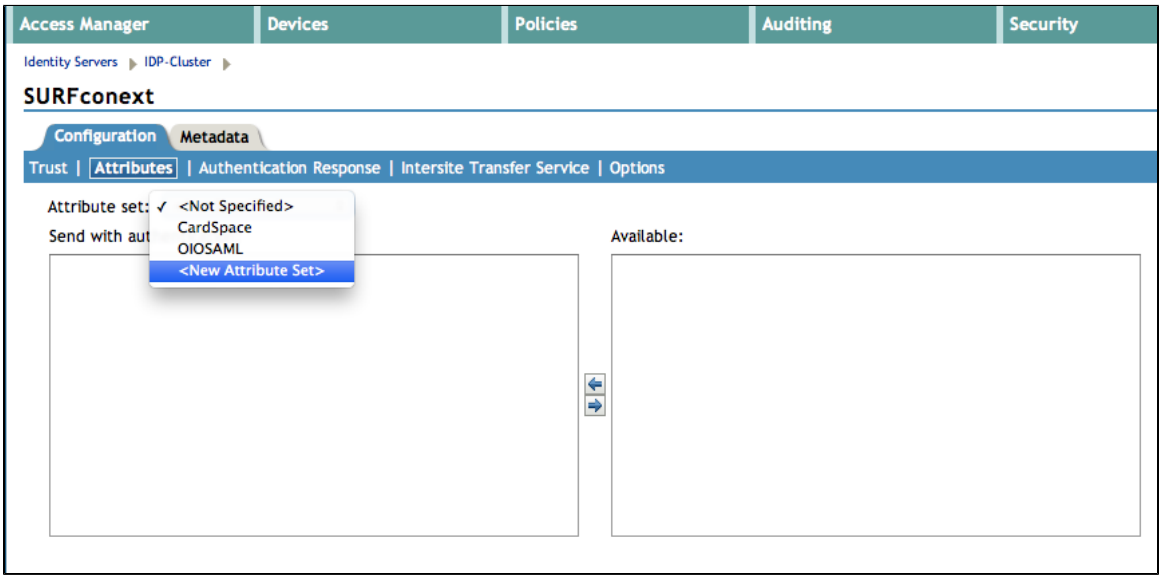
2. Geef deze URL door aan het SURFconext-team (support@surfconext.nl) en wacht op bericht waarin het SURFconext-team aangeeft dat de metadata is geconfigureerd. Je kunt intussen wel verder met de overige stappen, behalve de laatste controle.

5. Maak een attributen set aan

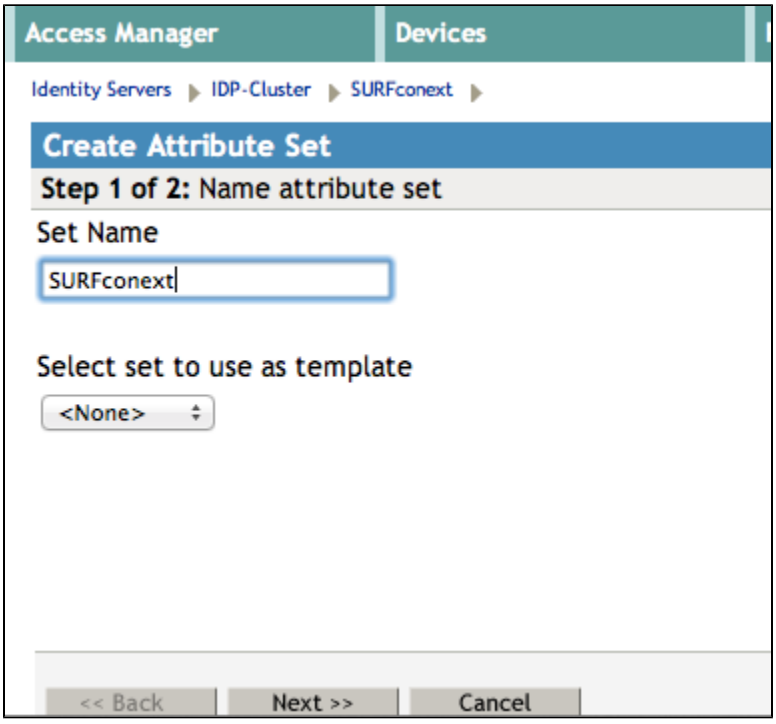
1. Ga naar 'Devices' -> 'Identity Servers' -> 'IDP-cluster'.

2. Ga naar de tab 'SAML 2.0'. Klik op de zojuist aangemaakte Service Provider.

3. Klik in de tab 'Configuration' op 'attributes' en kies bij het uitrolmenu 'attribute set' voor '<New Attribute Set>'. Zie hieronder in de figuur:



4. Geef de nieuwe attributenset een naam, zoals in onderstaand figuur.



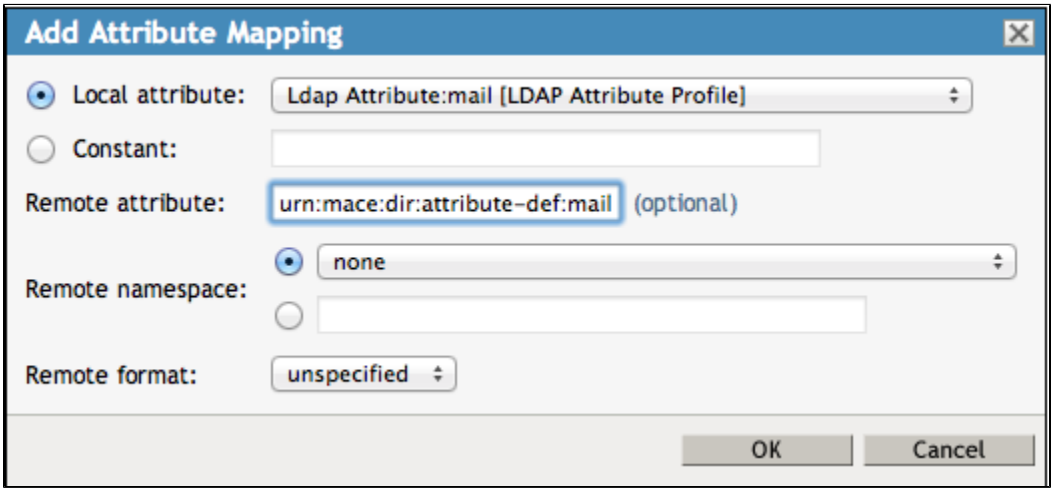
Klik op 'Next' en vervolgens in het volgende scherm op 'New'.

Voor SURFconext zijn conform Vereiste attributen volgende attributen verplicht:

```
urn:mace:dir:attribute-def:mail
urn:mace:dir:attribute-def:displayName
urn:mace:dir:attribute-def:cn
urn:mace:dir:attribute-def:sn
urn:mace:dir:attribute-def:givenName
urn:mace:terena.org:attribute-def:schacHomeOrganization
urn:mace:dir:attribute-def:uid
urn:mace:dir:attribute-def:eduPersonPrincipalName
urn:mace:dir:attribute-def:eduPersonAffiliation
urn:mace:dir:attribute-def:eduPersonScopedAffiliation
```

De betekenis van deze attributen is te vinden op de attributenschema pagina van SURFconext. Zie Attributen in SURFconext (NL).

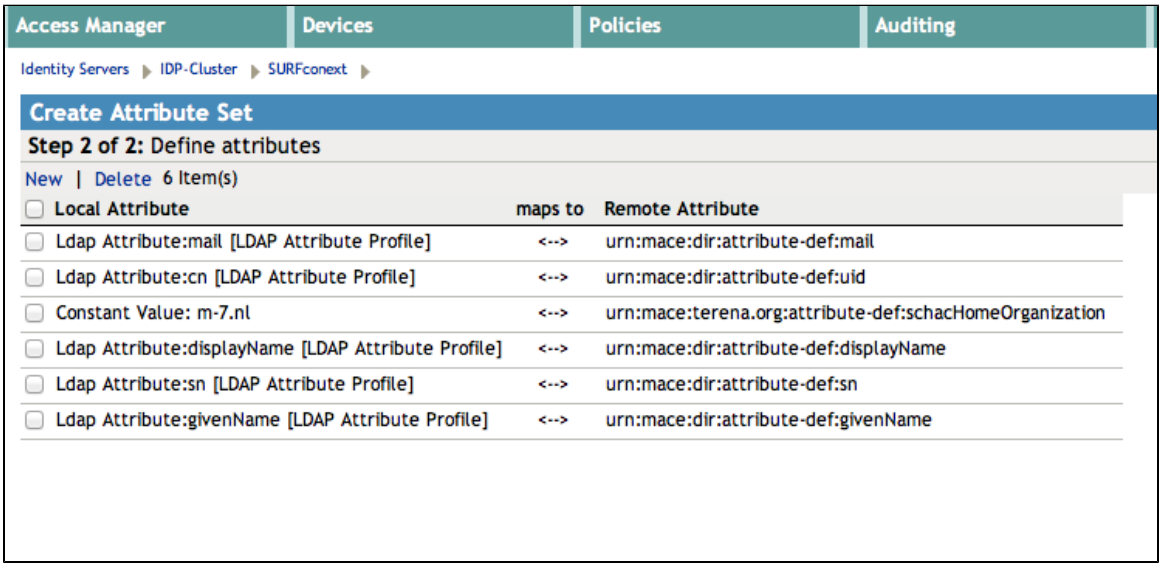
5. Kies in het scherm hieronder voor de local attribute-waarde. Let erop dat je voor de meeste attributen een naam moet kiezen die in LDAP voorkomt (aangegeven met 'LDAP Attribute'). Vul voor 'remote attribute' de volledige urn in zoals gespecificeerd in het attributenschema van SURFconext.



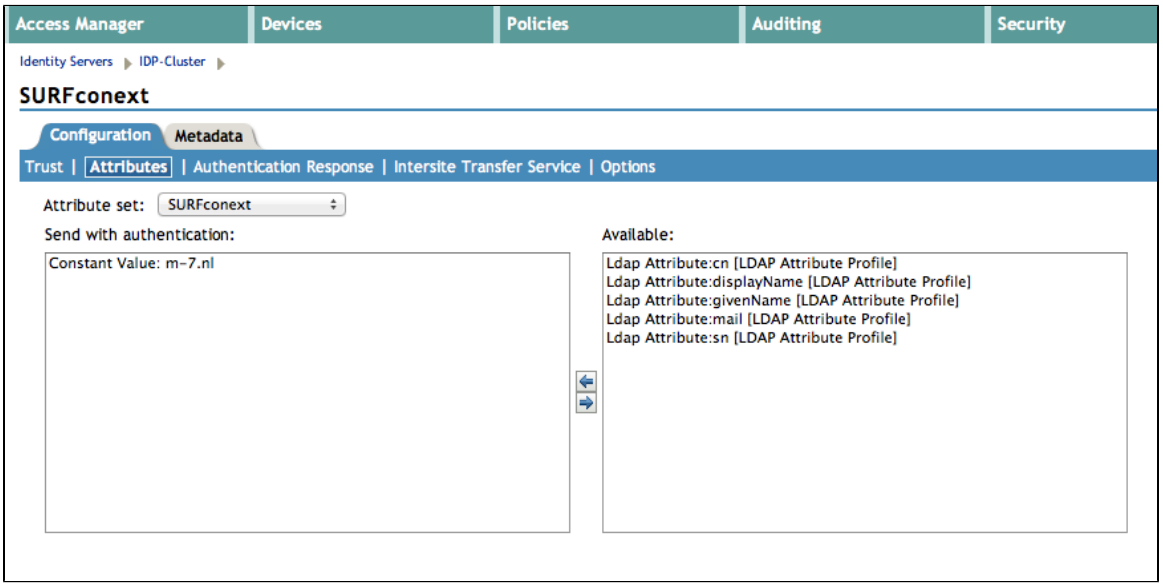
6. Klik op 'OK' en herhaal dit voor de overige attributen.

> ⚠ Kies de attributen mapping zorgvuldig en correct. Je moet dus het locale attribuut bij `urn:mace:dir:attribute-def:mail` voor iedereen daadwerkelijk wijzen in een geldig e-mailadres.
>
> Voor schacHomeOrganization moet je een 'Constant' kiezen met als waarde de domeinnaam van de Identity Provider. In ons geval 'm-7.nl'.
>
> Bij een standaardinstallatie van eDirectory die wordt gebruikt als User Store wordt meestal niet 'uid' gebruikt als inlognaam maar 'cn'. Map daarom het LDAP-attribuut 'cn' op `urn:mace:dir:attribute-def:uid`.

Het resultaat hiervan zie je in onderstaand figuur.



7. Klik op 'Next'. Je kunt kiezen welke attributen uit de set je wilt gebruiken. Zie de figuur hieronder:



In bovenstaand voorbeeld moeten alle attributen links komen te staan (bij 'Send with authentication').

8. Update de clusterconfiguratie zoals hierboven beschreven bij stap 4 van de paragraaf 'User store toevoegen'. Vergeet deze stap niet!

6. Test de configuratie

Nadat je van SURFnet bevestiging hebt ontvangen dat jouw metadata is toegevoegd, kun je jouw nieuwe Identity Provider-systeem testen op een test-Service Provider. Hiervoor heeft SURFnet de volgende URLs beschikbaar: https://engine.surfconext.nl/authentication/sp/debug en https://profile.surfconext.nl/.

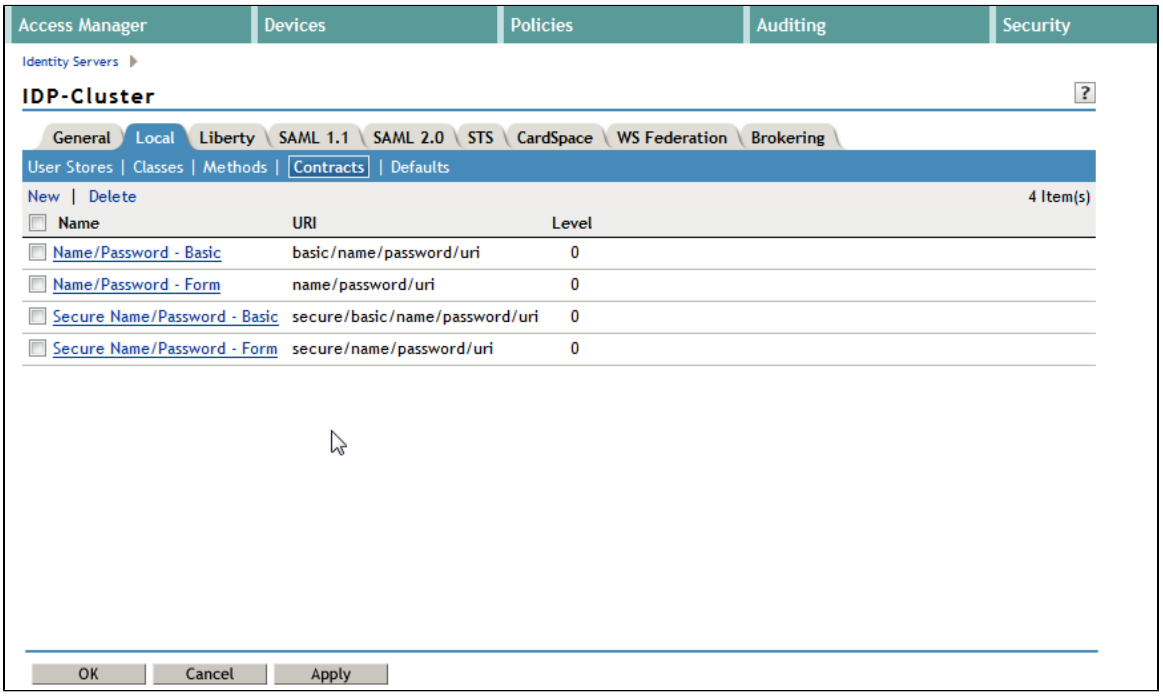
Je hebt een testkoppelling zolang je de bijlage bij het SURFnet-contract voor SURFconext nog niet ondertekend heb teruggestuurd naar SURFnet. Daarna heb je automatisch een productiekoppeling. Overigens zijn de URL's misschien aan verandering onderhevig. Deze moet je nog wel eerst bij SURFnet verifiëren.

Compatibiliteits problemen met diensten

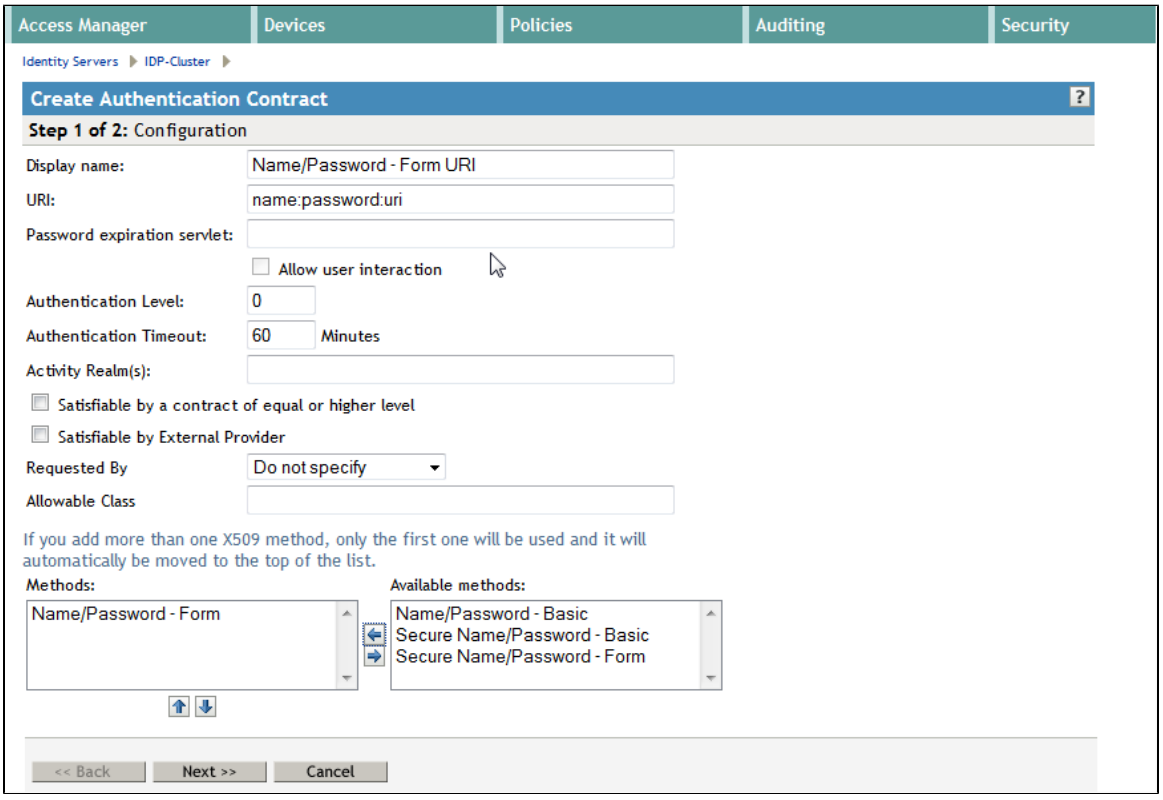
Het is bekend dat er compatibiliteitsproblemen zijn tussen NetIQ Access Manager en Service Providers die Microsoft (.NET) gebruiken. Deze problemen worden veroorzaakt door het anders interpreteren van de SAML2.0 specificatie. Volgens Microsoft kan een URI alleen een absolutie URI (zie wikipedia voor uitleg over URIs) zijn, terwijl NetIQ Access Manager ook gebruik maakt van URI verwijzingen (zoals ook mogelijk is volgens de SAML2.0 en XSD specificatie). Om deze problemen voor te zijn moet je het authenticatie contract van de NetIQ Access Manager Identity Provider aanpassen.

Als je het authenticatie contract wilt aanpassen om URI-verwijzingen te veranderen naar absolute URI's, dan moet je de volgende stappen doorlopen:

1. Ga naar 'Devices' -> 'Identity Servers' -> 'IDP-cluster'. Ga vervolgens naar de tab 'Local' en klik onder 'Contracts' op 'new' (zie onderstaand figuur).



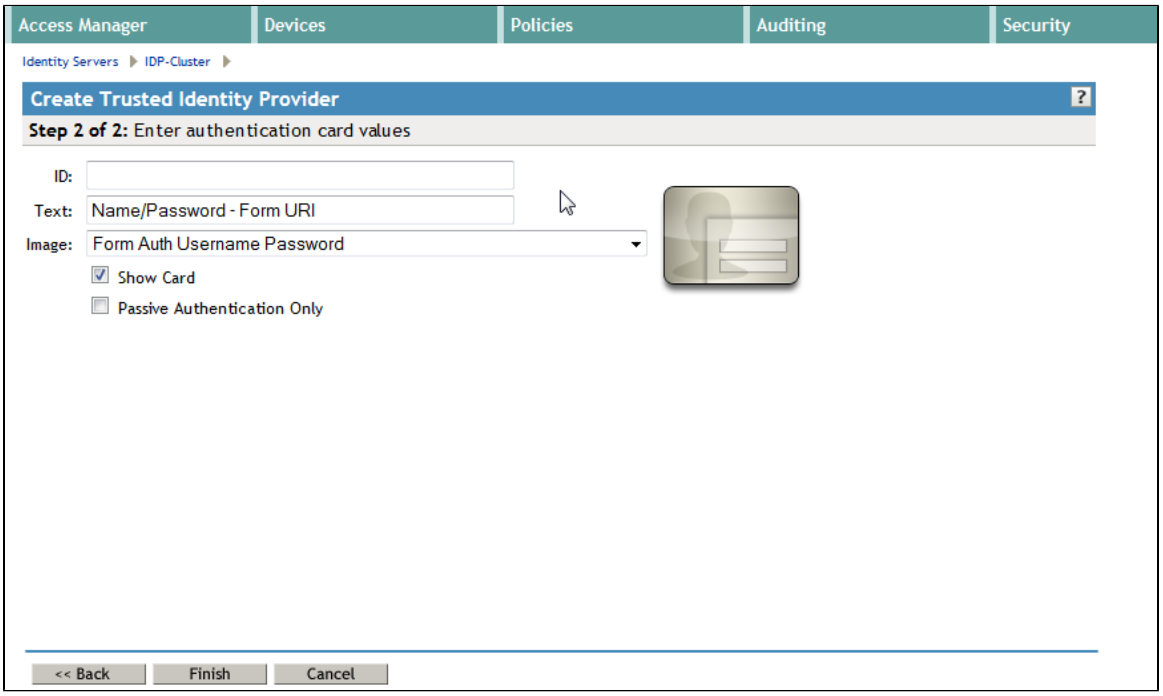
2. Vul de gegevens in zoals in het onderstaand figuur:



Vergeet niet de Method 'Name/Password - Form' aan te klikken en vervolgens op de  te klikken!

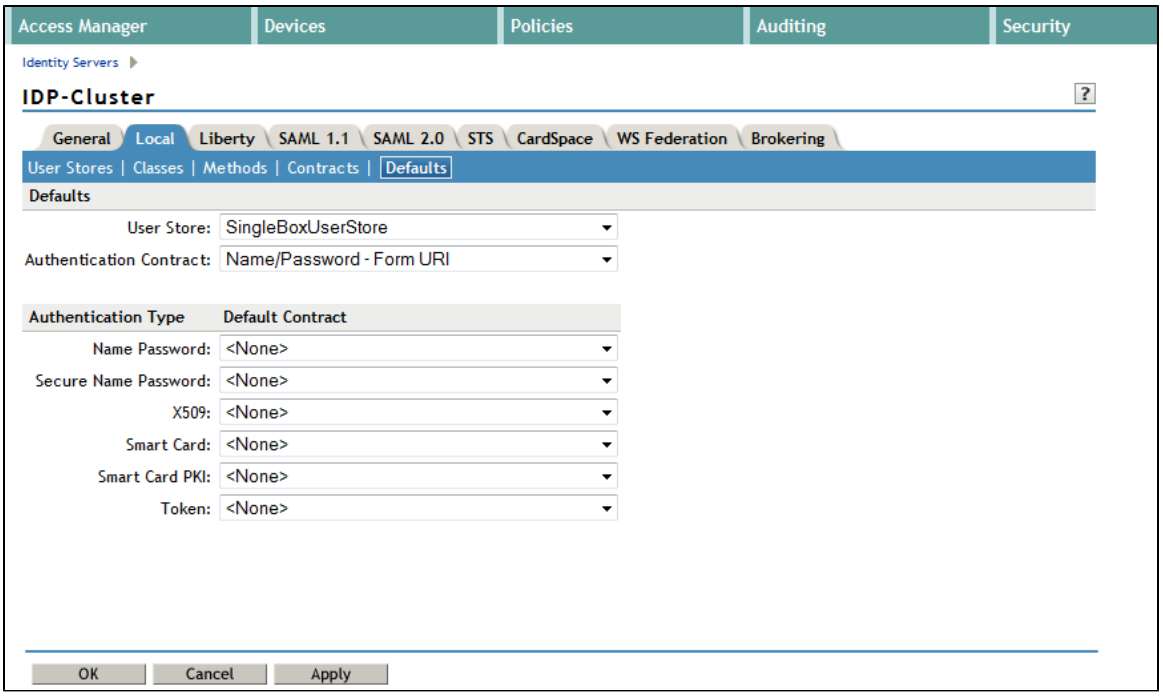
3. Klik op 'Next'.

4. Vul bij Text in: Name/Password - Form URI en selecteer bij Image: Form Auth Username Password (zie onderstaand figuur).



5. Klik op 'Finish'.

6. Stel nu deze nieuwe Authenticatie Contract in als de Default Authenticatie Contract. Dit doe je door naar het tabblad 'Defaults' te gaan. Vervolgens selecteer je bij Authentication Contract de nieuwe 'Name/Password - Form URI' contract (zie onderstaand figuur).



7. Klik op 'OK'.

8. Update de clusterconfiguratie zoals hierboven beschreven bij stap 4 van de paragraaf 'User store toevoegen'. Vergeet deze stap niet!